2026

Ongewenste kennis- en technologieoverdracht via kenniswerkers bij bedrijven

Verkenning naar nieuwe (beleids)maatregelen – rapportage januari 2026

Ministerie van Economische Zaken

Inhoud

1. Inleiding en probleemanalyse

1.1. Aanleiding

Het Dreigingsbeeld Statelijke Actoren 2 (DBSA 2)[1] omschreef in 2022 hoe staten op grote schaal activiteiten ondernemen om kennis en technologie in Nederland te verwerven, onder andere vanwege de sterke overlap die er bestaat tussen de inlichtingenbehoeften van verschillende statelijke actoren en de kennis en technologiesectoren waarin Nederland wereldwijd tot de koplopers behoort. Het jongste DBSA[2], verschenen in juli 2025, laat zien dat de dreiging van ongewenste overdracht van kennis en technologie onverminderd hoog blijft. Dit maakt niet alleen andere landen militair sterker, maar op de langere termijn kan hiermee de koplooperspositie van Nederland in bepaalde technologische domeinen teruglopen of kan het concurrerend vermogen van Nederlandse bedrijven afnemen.

Statelijke actoren gebruiken verschillende methoden om kennis en technologie te verwerven, zowel in de academische als private sector. Dat kan openlijk gebeuren, bijvoorbeeld in de vorm van bedrijfsovernames en talentrekrutering. Of dit kan illegaal plaatsvinden, bijvoorbeeld door middel van spionage. Dit laatste is een methode om informatie te verkrijgen voor economische, politiek-bestuurlijke en militaire doeleinden, maar kan ook worden ingezet om zicht te houden op de diaspora en dissidenten. Spionage gebeurt digitaal, maar ook via menselijke bronnen. Het gaat hierbij om personen die werkzaam zijn op strategische posities, in vitale sectoren, of die toegang hebben tot relevante (persoons)data.

1.2. Het versterken van onze kennis- en technologiepositie

Het beschermen (*protect*) van kennis en technologie is een belangrijk onderdeel van het economisch veiligheidsbeleid. Tegelijkertijd is het versterken (*promote*) van de Nederlandse kennis- en technologiepositie ook van belang voor de nationale veiligheid. Het DBSA 2025 laat zien dat er een mondiale *techrace* gaande is, tussen met name de Verenigde Staten en China, en dat steeds meer landen een protectionistisch economisch beleid voeren met handelsbarrières en beperking van handel in technologische kennis en goederen. Nederland en de Europese Unie raken in steeds meer technologiegebieden achterop, wat risico's oplevert voor onze veiligheid en economie en waarbij risicovolle strategische afhankelijkheden ontstaan. Met de Nationale Technologiestrategie (NTS)[3] heeft het kabinet de bouwstenen gelegd om innovatie te stimuleren, de positie van Nederland als technologisch leider te versterken en daarmee de technologische soevereiniteit van Nederland te waarborgen. Een van de randvoorwaarden om de doelen uit de NTS te kunnen halen is het aantrekken, behouden en doorontwikkelen van (top)talent, op alle niveaus. (Technisch) talent is echter schaars en het tekort aan technisch personeel vormt een structureel risico voor de opschaling van de defensie en veiligheidsindustrie[4]. Dit maakt de opgave in deze verkenning complex: maatregelen dienen een balans te vinden waarbij risico's op ongewenste kennisoverdracht via kenniswerkers kunnen worden gemitigeerd, zonder een belemmerende factor te worden voor het aantrekken van talent en het behalen van de NTS-doelstellingen.

1.3. Doel verkenning

In een eerste quickscan (zie bijlage 1) heeft het ministerie van Economische Zaken maatregelen, gericht op de kennismigrantenregeling, onderzocht om risico's op ongewenste kennis- en technologieoverdracht bij het bedrijfsleven te mitigeren. Het merendeel van de maatregelen zou

[1] Dreigingsbeeld Statelijke Actoren 2 | Nationaal Coördinator Terrorismebestrijding en Veiligheid
[2] Dreigingsbeeld Statelijke Actoren (DBSA) 2025 | Nationaal Coördinator Terrorismebestrijding en Veiligheid
[3] Kamerstuk 33 009, nr. 140, bijlage
[4] Kamerstuk 29 544, nr. 1283

gekoppeld zijn aan vreemdelingenwetgeving die internationale kenniswerkers toegang geven tot Nederland of de Nederlandse arbeidsmarkt, of zocht aansluiting bij andere bestaande relevante wet- en regelgeving. Na het opleveren van de quickscan zijn er nieuwe ontwikkelingen geweest die erop wezen dat het invoeren van maatregelen alleen gericht op derdelanders juridisch te kwetsbaar is. Beleid dient in deze context landenneutraal te zijn. Deze inzichten volgen ook uit het traject van het wetsvoorstel screening kennisveiligheid van OCW en de adviezen die daar zijn gegeven door het College van de Rechten van de Mens en de Landsadvocaat[5] en is tevens een van de uitgangspunten van de kabinetsaanpak Economische Veiligheid (EV).[6]

Hoewel mitigerende maatregelen niet direct kunnen worden gekoppeld aan arbeids- en verblijfsregelingen, blijft de noodzaak om risico's op ongewenste kennis- en technologieoverdracht te verminderen. Daarom is in april 2025 een nadere verkenning gestart, met deze rapportage als uitkomst. Doel van de verkenning is om te kijken of via andere wegen dan arbeids- en verblijfsregelingen, maatregelen kunnen worden toegepast om risico's op ongewenste kennisoverdracht te mitigeren.

Tot slot, machtsverhoudingen veranderen in hoog tempo, de internationale veiligheidssituatie is de afgelopen jaren sterk verslechterd en een open en op voorspelbare regels gebaseerde wereldeconomie is niet langer vanzelfsprekend. In dat kader is economische veiligheid uitgegroeid tot een eigenstandig beleidsterrein, waarbij Nederland inmiddels behoort tot de voorlopers in Europa.[7] Het is belangrijk om de uitkomsten van dit vervolg op de quickscan een plek te geven in het bredere en verstevigde EV-beleid en risico's op het weglekken van kennis via personeel bij bedrijven hierin integraal mee te nemen.

2. Kabinetsaanpak Economische Veiligheid

De verkenning is onderdeel van de bredere kabinetsaanpak Economische Veiligheid. Hiermee maken we onze economie weerbaar tegen de inzet van economische activiteiten of instrumenten die een risico voor onze nationale veiligheid vormen. De beleidsaanpak is gericht op drie hoofddoelen, namelijk:

- Het tegengaan van ongewenste kennis- en technologieoverdracht;
- Het borgen van continuïteit van vitale processen;
- Het verminderen en voorkomen van risicovolle strategische afhankelijkheden.

Naar analogie van het EU-kader vereist het realiseren van de doelstellingen een geïntegreerde aanpak langs drie sporen: *protect* (beschermen), *promote* (versterken) en *partner* (samenwerken), die worden versterkt door actieve ondersteuning van het bedrijfsleven en kennisopbouw op dit thema.

De verkenning is onderdeel van de *protect* initiatieven en richt zich primair op het mitigeren van risico's op het weglekken van sensitieve kennis en technologie. De maatregelen die onderdeel zijn van dit traject worden in samenhang bekeken met soortgelijke initiatieven die risico's op ongewenste kennis- en technologieoverdracht mitigeren. Dit zijn onder andere, maar niet uitsluitend, de pilot Erkend Referentschap (AenM), het wetsvoorstel screening kennisveiligheid (OCW), de Wet veiligheidstoets investeringen, fusies en overnames (Wet Vifo, EZ) en verschillende initiatieven die als onderdeel van de EV-campagne op 1 oktober jl. zijn gelanceerd. Het geheel aan maatregelen dient voldoende in te spelen op de toenemende dreiging, waarbij ook zal moeten worden afgewogen wat acceptabele risico's zijn en toename van onder meer regeldruk. Veiligheidsrisico's kunnen immers nooit volledig worden afgedekt.

---

[5] Overheid.nl | Consultatie Wet screening kennisveiligheid

[6] Kamerstuk 30 821, nr. 302

[7] Clingendael en SEO (2025): Verkenning_Internationaal_EV_Instrumentarium.pdf p.92.

Bij de afweging tussen de verschillende beleidsmaatregelen in deze verkenning zullen de uitgangspunten van de kabinetsaanpak worden gevolgd. Die luiden als volgt:

- Het instrumentarium bevindt zich primair op nationaal niveau, waarbij een toenemende coördinatie en samenwerking in Europees en internationaal verband de inzet versterkt. Het kabinet streeft daarom bij maatregelen op het gebied van economische en kennisveiligheid naar samenhang op EU- en internationaal niveau. Dit komt de effectiviteit van maatregelen ten goede en is belangrijk voor een gelijk speelveld;
- Het beleid is landenneutraal, conform internationale principes, rechtsbeginselen en verplichtingen zoals het non-discriminatiebeginsel;
- Het beleid is adaptief en risicogebaseerd, om de nationale veiligheidsbelangen zo goed mogelijk te waarborgen en marktverstoring te minimaliseren.

3. Maatregelen

3.1. De basis

Het mitigeren van risico's op ongewenste kennisoverdracht vraagt van bedrijven niet enkel maatregelen gericht op personeelsbeleid, maar een aanpak waarbij integraal wordt gekeken hoe risico's op het weglekken van kennis binnen de verschillende facetten van de bedrijfsvoering kunnen worden gemitigeerd. Concreet betekent dit dat een integrale set maatregelen binnen een bedrijf nodig is die zich onder andere richt op:

- Beveiliging van de digitale werkomgeving
- Beveiliging van de fysieke werkomgeving
- Organisatie en bestuur
- Personeelsbeleid

Maatregelen gericht op personeelsbeleid vormen hier het sluitstuk. Immers: stel dat personeel wordt gescreend, maar gevoelige (technologische) kennis onvoldoende is beveiligd, dan ondermijnt dit de effectiviteit van de screening. Dit werkt ook andersom: indien informatie voldoende wordt beveiligd, maar personen kunnen zonder voorwaarden toegang krijgen, dan ondermijnt dit de effectiviteit van de (fysieke en digitale) beveiliging van sensitieve kennis. Daarmee geldt ook dat volgordelijkheid in de implementatie van maatregelen van belang is. Bedrijven dienen allereerst hun intellectueel eigendom (waardevolle bezittingen, technologie, kennis, processen en data) te identificeren, beveiligen en compartimenteren, voordat maatregelen gericht op personeelsbeleid effectief kunnen worden ingericht. Daarvoor is het immers noodzakelijk om te weten wie toegang krijgt tot sensitieve kennis en technologie binnen het bedrijf en wat die betreffende kennis is.

3.2. Beleidsmatig instrumentarium

Voor de inzet van beleid zijn grofweg drie mogelijkheden te onderscheiden, variërend van bewustwording en ondersteuning (beleidsimpulsen) tot wet- en regelgeving. In deze verkenning wordt onderzocht welk van deze instrumenten (of een combinatie daarvan) het uitgangspunt kan vormen voor eventueel nieuw of aangepast beleid binnen de brede Kabinetsaanpak EV, zoals omschreven in paragraaf 2. De bevindingen van de verkenning worden in het volgende hoofdstuk schematisch weergegeven en komen samen in de daaropvolgende conclusies.

1. Beleidsmaatregelen gericht op bewustwording, ondersteuning van en samenwerking met het bedrijfsleven
Aard van de maatregel: vrijwillig **Doelgroep:** bedrijven die actief zijn op het gebied van sensitieve technologie en andere

organisaties in het ecosysteem (denk aan brancheorganisaties, investeerders, coalities etc.).

Omschrijving: op 1 oktober jl. is de campagne 'Bescherm wat je sterk maakt' gelanceerd. Onderdeel van deze campagne zijn onder andere de website Maakjebedrijfweerbaar.nl en de uitbreiding van het Ondernemersloket Economische Veiligheid. Via de website vinden bedrijven praktische hulpmiddelen, richtlijnen en andere betrouwbare informatie om stappen te kunnen zetten op het gebied van veiligheid. Personeelsbeleid is hierbij integraal meegenomen in de verschillende tools en informatiebronnen.

De komende periode wordt verder verkend welke aanvullende, gerichte initiatieven nodig zijn om bedrijven bewust te maken van de risico's op (fysieke) spionage en waar nodig te ondersteunen bij het mitigeren van dergelijke risico's. De insteek is om hierbij nauw samen te werken met partijen in het ecosysteem die dichtbij het bedrijfsleven staan. Denk bijvoorbeeld aan brancheorganisaties, regionale ontwikkelingsmaatschappijen, investeerders en andere relevante coalities. Daarbij zal worden gemonitord wat de voortgang is voor wat betreft de implementatie van veiligheidsmaatregelen onder het bedrijfsleven.

2. Randvoorwaarden bij overheidssubsidies

Aard van de maatregel: randvoorwaardelijk
Doelgroep: bedrijven die financiering ontvangen van de ministeries EZ/ KGG/ LVVN voor initiatieven op het gebied van sensitieve technologie (nader te specificeren, wordt opgepakt in separate verkenning).

Omschrijving: de ministeries stimuleren innovatie onder andere door middel van financiering. Dit kan mogelijk leiden tot verhoogde interesse van statelijke actoren in bepaalde initiatieven. Daarom wordt in een separate verkenning onderzocht welke risico's zich voordoen op het weglekken van kennis (via project of bedrijf) bij overheidssubsidies voor sensitieve technologieën en in hoeverre deze proportioneel gemitigeerd kunnen worden, bijvoorbeeld door randvoorwaarden te stellen aan de ontvangende partij van de subsidie. Dit is onderdeel van een bredere verkenning die EZ uitvoert, zoals aangekondigd in de voortgangsbrief Kabinetsaanpak Economische Veiligheid, en waarbij wordt onderzocht of en welke EV risico's zich voordoen bij subsidies die de ministeries aan het bedrijfsleven verstrekken.

3. Wet- en regelgeving

Aard van de maatregel: verplichtend
Doelgroep: bedrijven die actief zijn op het gebied van sensitieve technologie

Omschrijving
Bedrijven kunnen middels wet- en regelgeving worden verplicht om veiligheidsmaatregelen te integreren in hun bedrijfsvoering. Daarin zijn grofweg twee mogelijkheden te onderscheiden:

<u>3A: wettelijke inspanningsverplichting</u>
In een wet wordt een zorgplicht (het mitigeren van risico's op het weglekken van kennis) geformuleerd waar bedrijven aan moeten voldoen, inclusief bijbehorende minimale inspanningen (maatregelen) die van bedrijven worden verwacht. Bedrijven zijn hierbij zelf verantwoordelijk voor de uitvoering van deze maatregelen.

<u>3B: screeningswet</u>
Met dit wetsvoorstel zou een screeningsplicht worden geïntroduceerd voor eenieder die werkzaamheden uitvoert waarbij toegang kan worden verkregen tot sensitieve technologie. De screening van personeel dat toegang heeft tot sensitieve (technologische) kennis binnen het bedrijf wordt uitgevoerd door een overheidsinstantie. Bedrijven blijven zelf

verantwoordelijk voor de implementatie van maatregelen gericht op bijvoorbeeld de digitale en fysieke beveiliging van hun werkomgeving.

4. Bevindingen

4.1. Doelgroepafbakening

Idealiter ziet een aanpak toe op een zo specifiek mogelijk doelgroep. Voor het wetsvoorstel screening kennisveiligheid van OCW was het oorspronkelijke voornemen om onderzoekers en (master)studenten uit derde landen te screenen voorafgaand aan en met het oog op een verblijfsrechtelijke procedure. De adviezen van het College van de Rechten van de Mens en de Landsadvocaat hierover gaven OCW aanleiding om dit voornemen te herzien, omdat het maken van onderscheid op basis van nationaliteit niet kon worden toegepast om de doelgroep van de screening af te bakenen. OCW heeft de doelgroep aangepast naar onderzoekers en (master)studenten die toegang kunnen krijgen tot sensitieve kennis of technologie op een Nederlandse kennisinstelling, ongeacht nationaliteit of verblijfsrecht. Hiermee bestaat niet langer het risico op (indirecte) discriminatie.

De juridische afdeling van het ministerie van Economische Zaken (WJZ) en juridisch adviseurs van het ministerie van Asiel en Migratie (gespecialiseerd in het vreemdelingenrecht) hebben geadviseerd dat de uitgangspunten uit het advies van de Landsadvocaat en het College van de Rechten van de Mens omtrent de doelgroepkeuze van het wetsvoorstel screening kennisveiligheid ook relevant zouden zijn in een EZ-wetstraject gericht op kenniswerkers bij bedrijven. Een doelgroepafbakening waarbij maatregelen enkel zijn gericht op derdelanders is juridisch gezien te kwetsbaar. Ook hier geldt dat onderscheid wordt gemaakt tussen twee groepen die zich in een vergelijkbare positie bevinden:

1) Enerzijds derdelanders die naar Nederland komen om te werken bij een bedrijf actief op het gebied van (zeer) sensitieve technologie;
2) Anderzijds derdelanders die met een ander verblijfsdoel al in Nederland verblijven en dan pas besluiten te gaan werken bij een bedrijf actief op het gebied van (zeer) sensitieve technologie.

Ook als het gaat om de doelgroepafbakening van derdelanders ten aanzien van de Unieburgers, is het aannemelijk dat de voorgenomen doelgroepafbakening een objectieve rechtvaardiging behoeft, omdat onderscheid wordt gemaakt naar nationaliteit en/of verblijfsstatus, dan wel omdat een rechtvaardiging nodig is gelet op de naleving van het algemene gelijkheidsbeginsel. Indien er sprake is van gelijke gevallen waartussen onderscheid wordt gemaakt, dan is de volgende stap om na te gaan of een redelijke en objectieve rechtvaardiging bestaat vanwege de verschillen die bestaan tussen die twee gevallen. Een solide beleidsmatige onderbouwing hiervoor is moeilijk te vinden. Dit komt omdat, kijkend naar de dreigingsbeelden, risico's voor de nationale veiligheid kunnen uit gaan van personen van alle nationaliteiten en ongeacht de verblijfstatus.

Concluderend dat het risico van (indirecte) discriminatie op basis van nationaliteit en/ of verblijfsprocedure beperkt zou moeten worden, betekent dit dat de doelgroep van deze verkenning als volgt is:

- Op bedrijfsniveau betreft dit in Nederland gevestigde bedrijven die actief zijn op het gebied van (zeer) sensitieve technologie. Hierbij wordt de afbakening van de Wet Vifo en de voorgenomen uitbreiding van het betreffende toepassingsbereik gevolgd, dit is de meest adequate schatting die beschikbaar is binnen de pijler 'ongewenste kennis- en technologieoverdracht' van het kabinetsbrede EV-beleid. Dit betekent dat naar schatting 1750 – 3190 bedrijven vallen onder de doelgroep van deze verkenning;

- Binnen deze bedrijven behoren tot de doelgroep medewerkers die toegang hebben tot sensitieve kennis- en technologie (m.n. kenniswerkers, maar bijvoorbeeld ook technisch ondersteunend personeel). Dit betreft naar schatting enkele tienduizenden kenniswerkers.

Er is gekozen om de doelgroep zoveel als mogelijk aan te sluiten op de afbakening die onder de Wet vifo is gemaakt, omdat voor bedrijven die onder deze reikwijdte vallen, geldt dat er sprake is van risico's op ongewenste kennis- en technologieoverdracht. Zij zouden logischerwijs ook onder eventuele wet- en regelgeving gericht op personeelsbeleid vallen, zoals een mogelijke zorg- of screeningsplicht.

Omvang doelgroep en risicogerichte aanpak
De uitvoerbaarheid en proportionaliteit van eventuele wet- en regelgeving (zoals een screeningsplicht) staan mede onder druk vanwege de omvang van de doelgroep (zie ook paragraaf 4.4 over effectiviteit, uitvoerbaarheid en proportionaliteit). Er is de afgelopen maanden onderzocht of het mogelijk is om bovenstaande doelgroep in te perken ten behoeve van een meer risicogerichte aanpak, bijvoorbeeld door te prioriteren tussen en binnen technologiesectoren op basis van de dreiging. De diensten hebben aangegeven dat dreigingsinformatie slechts in beperkte mate bruikbaar is bij het opstellen van een doelgroepafbakening als er geen scherpe afweging vooraf is gemaakt over de te beschermen belangen.

Het inrichten van een risicogerichte aanpak is ook complex, omdat EZ vooralsnog onvoldoende zicht heeft op het gehele speelveld en waar de risico's zich precies bevinden. Dit is mede het gevolg van de omvang van het veld, de vele partijen die in de keten een rol spelen en het feit dat bedrijven hun bedrijfsactiviteiten aanpassen bijvoorbeeld in het licht van maatschappelijke uitdagingen (en daarmee bewegen tussen activiteiten die wel of niet als sensitief kunnen worden aangemerkt). Bovendien gaan technologische ontwikkelingen ook snel. Waar een technologie vandaag als niet sensitief kan worden bestempeld, kan door een doorbraakinnovatie deze al snel als (zeer) sensitief worden aangemerkt. Ook dit bemoeilijkt de inrichting van een risicogerichte aanpak op medewerkersniveau binnen bedrijven. Dit aandachtspunt is ook door het Verenigd Koninkrijk (VK) opgemerkt in het kader van de internationale benchmark. Als onderdeel van het kennisveiligheidsbeleid van het VK kunnen studenten en onderzoekers aan kennisinstellingen gescreend worden door een overheidsinstantie. Het VK heeft onlangs een review uitgevoerd over dit beleid, waarbij geconstateerd wordt dat de dreigingen dermate snel evolueren dat de genomen interventies soms moeite hebben om de technologische ontwikkelingen bij te benen.

4.2. WAT DOET HET BEDRIJFSLEVEN ZELF EN WAAR IS BEHOEFTE AAN?

Brede EV-maatregelen
De recent gepubliceerde studie van Clingendael ('Hoe Nederlandse bedrijven omgaan met economische veiligheid) en de gesprekken die met vertegenwoordigers van het bedrijfsleven tijdens deze verkenning zijn gevoerd, geeft op hoofdlijnen het volgende beeld van of en hoe bedrijven economische veiligheid integreren in hun organisatie en keten:

- De helft van de Nederlandse bedrijven die actief zijn in sleuteltechnologieën of vitale processen of diensten leveren zijn nog weinig bekend met het concept 'economische veiligheid'
- Hoewel 9 van de 10 bedrijven risico's zien op het gebied van economische veiligheid, investeren zij nog lang niet allemaal in de aanpak daarvan;
- De belangrijkste belemmerende factoren hierbij zijn de kosten, tijdsinvestering en het gebrek aan kennis en expertise;

- Handelingsperspectieven voor de overheid en het bedrijfsleven zijn (onder andere, maar niet uitsluitend);
    - Investeren in grotere kennis van EV-instrumenten onder bedrijven, ondersteunen van het bedrijfsleven bij het nemen van EV-maatregelen, investeren in nauwe samenwerking met sectoren (o.a. via beleidsstimulansen zoals belastingvoordelen) en samenwerking met sectorale ecosystemen en brancheorganisaties;
    - De helft van de bedrijven krijgt informatie over EV het liefst via bijeenkomsten van de brancheorganisaties. Voor advies over EV achten bedrijven de Nederlandse overheid veruit het meest betrouwbaar (75%). Brancheorganisaties en inlichtingendiensten blijken ook belangrijke bronnen van informatie (50% en 49%);
    - Wet- en regelgeving. Dit is een krachtig instrument om aandacht voor EV te bewerkstelligen bij bedrijven. Tegelijkertijd ervaren bedrijven veel (gevolgen) van regeldruk. Wet- en regelgeving zou in samenspraak met bedrijven kunnen worden verkend;
    - Investeren in een bredere 'promote-agenda' als aanvulling op ondersteuning van bedrijven bij de 'protect-agenda' van defensieve maatregelen. Het gaat hierbij om maatregelen die eigen capaciteiten en concurrentiekracht helpen behouden of vergroten.

<u>Maatregelen gericht op ongewenste kennisoverdracht en personeelsbeleid</u>
Als specifiek wordt ingezoomd op hoe bedrijven omgaan met risico's op ongewenste kennisoverdracht (via personeel), dan valt op dat bedrijven die economische veiligheid al hebben geïntegreerd een diversiteit aan maatregelen nemen gericht op verschillende aspecten van hun bedrijfsvoering. Dit gaat bijvoorbeeld om maatregelen op het gebied van personeelsbeleid (o.a. screening van personeel), beveiliging van de digitale en fysieke werkomgeving, compartimentering, en de inrichting van de organisatie (o.a. instelling van *security officers* en initiatieven om personeel te trainen en bewust te maken van veiligheidsrisico's). Bedrijven nemen deze maatregelen omdat ze een eigen verantwoordelijkheid hebben om hun kennis en technologie te beschermen, en daarmee hun intellectueel eigendom en verdienvermogen. Daarnaast zijn bedrijven via bestaande voorschriften en wet- en regelgeving reeds verplicht om specifiek aangewezen functies te laten screenen, bijvoorbeeld onder de Wet veiligheidsonderzoeken en onder de voorschriften van de Algemene Beveiligingseisen van Rijksoverheidopdrachten. Laatstgenoemde bouwt voort op bestaande beveiligingseisen die door het ministerie van Defensie worden gebruikt en zorgt voor meer bescherming en meer duidelijkheid bij bedrijven.

Bedrijven die relatief minder ver zijn met de implementatie van maatregelen hebben over het algemeen wel bewustzijn van EV-risico's, maar ze zoeken naar praktische en concrete handvatten om risico's te mitigeren. Startups zetten vooralsnog relatief het minst in op economische veiligheidsmaatregelen. Voor hen is een belangrijke eerste stap om intellectueel eigendom te ontwikkelen, te vermarkten en om het vervolgens te kunnen beveiligen en compartimenteren. Pas dan kan personeelsbeleid effectief worden ingericht. Hierbij is ondersteuning van de overheid wenselijk. Het implementeren van EV-beleid vraagt namelijk gerichte expertise, capaciteit en middelen. Dit is, gegeven de groeifase waarin startups zich bevinden, relatief gezien een aanzienlijke uitdaging voor dergelijke bedrijven.

Tot slot: door het bedrijfsleven is ook op het gebied van personeelsbeleid herhaaldelijk

aangestipt dat *protect* maatregelen vanuit de overheid (zoals screening) gepaard zouden moeten gaan met (voldoende) *promote* en *partner* maatregelen gericht op het aantrekken en behoud van talent. Dit helpt om personeelsbeleid op een verantwoorde manier in te kunnen richten en vermindert mogelijk negatieve neveneffecten op bijvoorbeeld de concurrentiepositie van bedrijven als het gaat om het aantrekken van talent. Hierbij kan worden gedacht aan het voorbeeld van het Verenigd Koninkrijk, waarbij studenten en onderzoekers aan kennisinstellingen kunnen worden gescreend door een overheidsinstantie (*protect* maatregel), maar waarbij er tegelijkertijd een *Global talent taskforce* met een budget van 54 miljoen pond is ingesteld om internationaal talent naar het Verenigd Koninkrijk toe te trekken (*promote* maatregel).

4.3. Internationaal speelveld

Doelstelling internationale benchmark
Het Ministerie van Economische Zaken heeft een benchmark uitgevoerd om te onderzoeken hoe andere landen omgaan met risico's op ongewenste kennis- en technologieoverdracht via kenniswerkers bij bedrijven. Het resultaat is een overzicht van selecte voorbeelden van instrumenten en maatregelen die deze landen overwegen en/of in uitvoering hebben om de genoemde veiligheidsrisico's te mitigeren. Dit overzicht is enerzijds bedoeld om het ministerie te inspireren bij de uitwerking en vormgeving van eventuele nieuwe (beleids)maatregelen. Anderzijds geven de resultaten een indruk in hoeverre eventueel nieuw beleid in Nederland van invloed kan zijn op de internationale concurrentiepositie van Nederlandse bedrijven, bijvoorbeeld als het gaat om het aantrekken van talent, en hoe het internationaal speelveld andersom van invloed kan zijn op de effectiviteit van Nederlandse instrumenten.

Aanpak
Het onderzoek is uitgevoerd op basis van kwalitatieve onderzoeksmethoden. De focus lag daarbij op een vragenlijst die is uitgezet onder de Economische veiligheidsposten (EV-posten) en Innovatieattachés (IA's) van het ministerie van Buitenlandse Zaken en/of Economische Zaken, aangevuld met online gesprekken. Daarnaast is er online deskresearch gedaan en is gebruik gemaakt van informatie – waar het ging over kennisveiligheidsbeleid – die is aangeleverd door het ministerie van Onderwijs, Cultuur en Wetenschap. De volgende landen waren onderdeel van de benchmark:

- Australië, Canada, Duitsland, Frankrijk, Japan, Taiwan, het Verenigd Koninkrijk, de Verenigde Staten, Zuid-Korea en Zweden.

Gegeven de doelen van de benchmark is de selectie van landen gebaseerd op een cross-check van eerdere studies en vergelijkingen:

- Een internationale vergelijking van het EV-instrumentarium van 11 landen door Clingendael;[8]
- De Monitor Ondernemersklimaat, waarin de positie van Nederland wordt vergeleken met een set van 11 referentielanden voor wat betreft de aanwezigheid van talent en het gemak waarmee bedrijven gekwalificeerde werknemers vinden[9].

De afweging van Nederland om een EV-post en IA op de ambassade in een bepaald land te stationeren, heeft ook een rol gespeeld in de selectie.

In het onderzoek zijn de volgende hoofdvragen gesteld:
1. Kent uw land beleid op het gebied van economische en/ of kennisveiligheid?

[8] Verkenning Toolkit Economische Veiligheid | Clingendael
[9] Kamerstuk 32 637, nr. 659, bijlage

2A. Kent uw land beleid – of wordt dit overwogen – om risico's op ongewenste kennisoverdracht bij bedrijven via kenniswerkers (spionage) tegen te gaan? Indien het antwoord 'ja' is, ga door naar vraag 3. Indien het antwoord 'nee' is, ga door naar vraag 2b.
2B. In sommige landen is er bewust voor gekozen om dergelijk beleid te ontwikkelen voor kennisinstellingen, maar (vooralsnog) niet voor bedrijven of andersom. In hoeverre is deze afweging ook in uw land gemaakt? En met welke motivering?
3. Kunt u inzicht geven in hoe dit beleid eruit ziet/ eruit gaat zien langs de lijnen van de vijf verdiepende vragen hieronder.

In de verdiepende vragen onder 3 is onder andere doorgevraagd naar concrete maatregelen, de doelgroep van deze maatregelen evenals de beleidsmatige/ juridische basis voor dit beleid, de verantwoordelijke instanties en de wijze van monitoring, evaluatie en verantwoording.

Resultaten
De benchmark geeft het volgende beeld van het internationaal speelveld:

- In de meeste landen is er aandacht voor de risico's op (fysieke) spionage in het bedrijfsleven. De maatregelen die worden getroffen, zijn met name gericht op bewustwording en ondersteuning van bedrijven. Dit resulteert onder andere in richtlijnen, taskforces (tools en kennisuitwisseling), consultatieservices, meldpunten, de inzet van *trade representatives* en de versterking van de samenwerking en informatiedeling tussen private en publieke organisaties.
- In een enkel land gelden strengere maatregelen, vaak voor een meer specifiek afgebakende doelgroep:
    - In Australië is er sinds 2024 nieuwe wetgeving waarbij aanvullende visumvereisten gelden voor derdelanders die actief willen zijn in een kritiek technologieveld (specifiek Public Interest Criterion 4003B)[10]. Het is hiermee mogelijk geworden om een visum te weigeren wanneer er een onredelijk risico bestaat op ongewenste overdracht van kritieke technologie. Ook kan een toegekend visum worden geannuleerd wanneer de minister van mening is dat er een risico bestaat op ongewenste overdracht van kritieke technologie.
- In enkele anderen landen worden ook personen bij het bedrijfsleven gescreend. De doelstelling en/ of doelgroep van deze wetgeving is anders dan in deze verkenning.
    - Op 9 oktober 2024 heeft Duitsland een wetsvoorstel goedgekeurd om veiligheidscontroles op personeel in kritieke sectoren van de staat en economie aan te scherpen en bedrijven te beschermen tegen spionage en sabotage. Het wetsvoorstel ziet toe op kritieke infrastructuurbedrijven (zoals spoorwegen en bevoorradingscentra) en de hoogste federale overheidsorganen;
    - Ook in Japan is, in aanvulling op bestaande wetgeving omtrent geheime overheidsinformatie, een nieuwe wet ingevoerd waarmee een veiligheidssysteem wordt opgezet voor vertrouwelijke economische informatie. Onderdeel van deze wet is ook een screeningsmechanisme. Deze is met name gericht op individuen werkzaam bij overheidsinstellingen, maar is ook van toepassingen op het bedrijfsleven. Economische informatie die hiermee wordt beschermd betreft bijvoorbeeld informatie over cyberaanvallen, fysieke aanvallen op kritieke infrastructuur of informatie verkregen van buitenlandse overheden via internationaal gezamenlijk onderzoek naar kritieke producten zoals halfgeleiders;

[10] Critical technology - enhanced visa screening measures.

    - Als onderdeel van het Franse kennisveiligheidsbeleid (*Protection du potentiel scientifique et technique technique de la nation,* PPST beleid) worden zogeheten veiligheidszones ingericht. Personen die toegang willen krijgen tot deze zones worden gescreend. Doel hiervan is om het wetenschappelijk en technisch potentieel van de natie te beschermen. Het PPST beleid is gericht op publieke en private onderzoeksinstellingen, (hoger) onderwijsinstellingen en het bedrijfsleven, waaronder 227 zgn. '*engineering schools'*. Deelname aan (lidmaatschap van) het PPST schema is gebaseerd op overleg tussen overheidsdiensten en de betreffende instantie.
- Zuid-Korea gaat (als onderdeel van het in december 2024 uitgevaardigde *5th Comprehensive Plan on Prevention of Divulgence and Protection of Industrial Technology*) de mogelijkheid tot screening van kennismigranten onderzoeken. Buitenlandse arbeiders vormen 3,8% van de Koreaanse arbeidsmarkt, waarbij het merendeel vooral actief is in sectoren als landbouw en horeca. Kennismigranten omvatten een zeer kleine fractie van de totale arbeidspopulatie;
- Opvallend is dat in meerdere landen – net als in Nederland[11] – het strafrecht is/ wordt geactualiseerd en uitgebreid om zo het weglekken van kennis en technologie naar een statelijke actor te kunnen bestraffen. Dit zou een preventief, afschrikwekkend effect moeten hebben. Dit geldt bijvoorbeeld in het geval van Canada, waar in 2024 een wet is aangenomen om buitenlandse inmenging tegen te gaan, waaronder strafbaarstellingen van het delen van militaire kennis- en technologie;
- Verschillende landen kennen een strenger kennisveiligheidsbeleid voor kennisinstellingen dan voor het bedrijfsleven. Tegelijkertijd groeien de zorgen over de bescherming van kennis en technologie bij bedrijven, met name als het gaat om startups, spinoffs en/ of MKB dat gelieerd is aan de academische wereld. In dat kader ontstaat langzaam een internationale discussie in hoeverre het kennisveiligheidsbeleid ook zou kunnen worden toegepast op de hiervoor genoemde type bedrijven. Specifiek komt terug dat:
    - Er in het Amerikaanse Congres zorgen zijn geuit over het weglekken van kennis via kleine kennisintensieve bedrijven – gelieerd aan de academische wereld en gefinancierd door de overheid - bijvoorbeeld via programma's zoals de *Small Business Innovation Research (SBIR)* en de *Small Business Technology Transfer (STTR);*
    - Canada en het Verenigd Koninkrijk met elkaar van gedachten hebben gewisseld of en hoe kennisveiligheidsbeleid geïmplementeerd kan worden in gevallen waar sprake is van startups of spin offs van academische samenwerking. Canada organiseerde in december 2025, als voorzitter van de G7, een G7+ evenement over kennisveiligheid waarin dit vraagstuk is geagendeerd. Vertegenwoordigers van het ministerie van Onderwijs, Cultuur en Wetenschap en Buitenlandse Zaken waren hierbij aanwezig;
    - De Europese Raad in mei 2024 een advies[12] uitbracht waarin zij lidstaten adviseerde hoe ze beleid rondom kennisveiligheid kunnen versterken en daarin beter kunnen samenwerken. Ook werd daarin geadviseerd om samen met de private sector richtlijnen op te stellen voor bedrijven die zich bezighouden met

[11] Vanaf 15 mei: meer vormen van spionage strafbaar | Nationaal Coördinator Terrorismebestrijding en Veiligheid
[12] Council adopts a recommendation to enhance research security - Consilium

onderzoek en innovatie, inclusief onderzoek intensieve startups, spinoffs en het MKB;
    - Tegelijkertijd wijst de Europese Raad ook op het volgende:
      '' Taking into account that a significant share of research and innovation takes place in the private sector, it should be stressed that, while the risks to which companies are exposed may be similar, their nature, needs and capacities differ from those of research performing organisations.''
- Tot slot: context is belangrijk. De aanwezigheid van talent, de rol die ecosysteempartijen spelen in kennis- en technologieontwikkeling, cultuur, geografische ligging en politieke context zijn voorbeelden van factoren die meespelen in de afweging om maatregelen wel of niet in te voeren en in welke vorm. Ter illustratie:
    - Geografisch: de nabijheid van een statelijke actor zoals China kan bepalend zijn voor het instrumentarium dat landen inzetten (bijv. het sluiten van regionale veiligheidspacts) of de doelgroep waar zij hun beleid op richten. Zo heeft Taiwan specifiek beleid gericht op het weglekken van kennis naar China en is dit ook voor Zuid-Korea aanleiding geweest om aanvullende beleidsmaatregelen te overwegen;
    - Aanwezigheid talent: schaarste aan talent (en de negatieve impact die dat heeft op industriële groei en technologische ontwikkelingen) spelen een rol in de afweging die landen maken voor de zwaarte waarmee *protect* maatregelen worden ingericht.

4.4. EFFECTIVITEIT, UITVOERBAARHEID EN PROPORTIONALITEIT

De inzet binnen beleidsinstrument 1 (bewustwording en ondersteuning, zie paragraaf 3.2.) zal verder worden geïntensiveerd door nauw samen te werken met ecosysteempartijen die dicht bij het bedrijfsleven staan. De verwachting is dat dit de effectiviteit van de EV-campagne ten goede zal komen, omdat zo een grotere doelgroep bereikt kan worden door partijen die het vertrouwen genieten van het bedrijfsleven. Het algemeen beeld is dat bedrijven zelf het belang delen dat hun kennis en technologie wordt beschermd. Het invoeren van veiligheidsmaatregelen kan – gezien andere bedrijfs- en innovatieprocessen, met name bij startups en het kleinbedrijf – echter ingewikkeld zijn, bijvoorbeeld door een tekort aan geschikt personeel in Nederland. Door samen te werken met de sector, oog te hebben voor de situatie waar zij zich in bevinden en van daaruit stap voor stap ondersteuning te bieden bij het invoeren van veiligheidsmaatregelen, is de verwachting dat dit een positieve bijdrage zal leveren aan de effectiviteit van de campagne.

Voor wat betreft instrument 2 (randvoorwaarden bij subsidies) geldt dat de komende maanden (als onderdeel van een bredere verkenning binnen de kabinetsaanpak EV gericht op subsidies) nader wordt verkend of en hoe EV-risico's gemitigeerd kunnen worden en hoe dat op effectieve, proportionele en uitvoerbare wijze kan worden ingericht. Personeelsbeleid wordt hierin meegenomen.

Voor wat betreft instrument 3 (wet- en regelgeving voor alle sensitieve technologiebedrijven) kan het volgende worden gezegd:

Effectiviteit
Het inrichten van effectief instrumentarium is in de praktijk complex. Instrumenten zijn vaak statischer dan de continu bewegende risico's. Het beleid zou daardoor (te) reactief van aard worden, wat de effectiviteit ervan bemoeilijkt. Daarom moet er altijd een verscheidenheid van instrumenten zijn die de effectiviteit van de totale aanpak vergroten.

Met betrekking tot de effectiviteit van pre-employmentscreening en screening door een

overheidsinstantie: bedrijven laten op dit moment als onderdeel van hun veiligheidsbeleid personeel screenen door commerciële organisaties. Indien wordt besloten om over te gaan op screening door een overheidsinstantie, moet worden afgewogen in hoeverre deze vorm van screening effectiever is en hoe een eventuele winst in effectiviteit zich verhoudt tot de bijkomende kosten en eventuele negatieve neveneffecten, zoals het bemoeilijken van de mogelijkheid van het bedrijfsleven om snel geschikt talent aan te trekken.

In dat kader moet worden opgemerkt dat het aannemelijk is dat een overheidsinstantie een reëler beeld van risico's kan schetsen indien een bepaald individu toegang wordt verleend tot sensitieve kennis. Immers kan een overheidsinstantie gebruikmaken van inlichtingen van de veiligheidsdiensten, in zoverre deze voorhanden is . Ook is er een risico is op een waterbedeffect, er zijn immers weinig tot geen landen die op deze schaal een vergelijkbare doelgroep screenen.

Beoogde uitvoeringslasten en uitvoerder (3b: screening door een overheidsinstantie)
Met een screening door een overheidsinstantie zijn verschillende kosten gemoeid. Dit betreft onder andere incidentele kosten zoals de ontwikkeling van een IT-structuur en andere voorzieningen voor de beoogd uitvoerder. Daarnaast geldt een gemiddelde kostprijs per screening. Ook zullen bedrijven zelf kosten moeten maken, bijvoorbeeld voor de digitale en fysieke beveiliging van hun kennis en technologie.

In het wetsvoorstel screening kennisveiligheid heeft OCW de kosten per screening ingeschat variërend tussen €1200 en €3000, met een gemiddelde kostprijs per screening van iets meer dan €1500. De kosten van een screening zijn afhankelijk van het feit of een eerstelijns onderzoek volstaat (wat voor circa 70% van de screenings wordt verwacht) of dat een nader onderzoek in de tweedelijn vereist is.[13]

Indien een nieuw screeningsmechanisme moet worden ingericht, zijn daar specifieke kosten aan gebonden. Daarbij is het echter moeilijk om in te schatten voor hoeveel screenings een eerste of tweedelijns onderzoek nodig is, omdat EZ onvoldoende zicht heeft op het speelveld en waar de risico's zich bevinden. Indien voor een eerste inschatting zou worden gekeken naar het kostenplaatje van OCW, dan zouden de kosten - uitgaande van de gemiddelde kostprijs en een doelgroep van enkele tienduizenden individuen - al snel kunnen oplopen tot tientallen miljoenen of hoger.

De aard en omvang van de doelgroep maken de centrale uitvoering van screening complex. De uitvoerbaarheid is afhankelijk van meerdere factoren (waaronder de voorgenomen opzet van het instrumentarium, de doelgroep, de capaciteiten en bevoegdheden van de beoogd uitvoerder, de informatievoorziening en samenwerking tussen beoogde ketenpartners etc.) en zal uiteindelijk daarop getoetst moeten worden. Gezien de omvang en complexiteit van het dossier, is het van belang dat de beoogd uitvoerder over relevante expertise en ervaring beschikt. Er waren daarbij twee partijen voorlopig in beeld. Uit gesprekken met hen blijkt het volgende:

- Het Bureau Toetsing Investeringen (BTI) – de instantie die binnen EZ belast is met uitvoerings- en handhavingstaken op het gebied van EV – beschikt over relevante expertise en ervaring, al zijn hun kernactiviteiten gericht op screening van eigendomsstructuren van bedrijven. Zij hebben wel ervaring met screening van individuen bij deze bedrijven, maar doen meer gespecialiseerde onderzoeken. Uitvoering van een lichte toets voor (in potentie) tienduizenden aanvragen past niet bij de functie en opzet van het BTI. Ook gezien de taken waar het BTI reeds mee belast is en

[13] Overheid.nl | Consultatie Wet screening kennisveiligheid, bijlage 'Wet'.

vele andere verzoeken die bij haar liggen, is het niet realistisch dat zij de screening van de beoogde doelgroep in dit traject op zich kan nemen;
- Ook Justis, onderdeel van het Ministerie van Justitie en Veiligheid, beschikt over relevante expertise en ervaring in het screenen van personen en in het screenen binnen het veiligheidsdomein. Justis breidt deze momenteel verder uit in haar rol als beoogd uitvoerder van het wetsvoorstel screening kennisveiligheid van OCW. Met de verdere opbouw van deze expertise kan Justis zeer waarschijnlijk op termijn een relevante bijdrage leveren op dit vraagstuk.

4.5. BELEIDSMATIG INSTRUMENTARIUM– JURIDISCHE ASPECTEN

Vanuit juridisch oogpunt is ook gekeken in hoeverre de in paragraaf 3.2 genoemde instrumenten op dit moment als juridisch houdbaar kunnen worden bestempeld. Voor wat betreft optie 1 (bewustwording en ondersteuning van het bedrijfsleven) geldt dat daar vooralsnog geen juridische implicaties in beeld zijn.

Voor wat betreft optie 2 (randvoorwaarden bij overheidssubsidies) geldt dat momenteel door EZ onderzoek wordt gedaan naar EV-risico's bij subsidieverlening, waarbij onder andere gekeken gaat worden naar risicomitigatie via aanvullende subsidievoorwaarden. Daarmee kan deze optie in vervolgstappen verder worden verkend en uitgewerkt indien andere maatregelen zoals bewustwording onvoldoende effect blijken te hebben.

Voor wat betreft optie 3 (wet- en regelgeving voor alle sensitieve technologiebedrijven) zal onder meer moeten worden onderbouwd dat wet- en regelgeving wenselijk en noodzakelijk is, en of de maatregel het beoogde doel op consistente wijze nastreeft en of dat niet met minder vergaande, niet-wettelijke middelen kan worden volstaan. Pas als minder vergaande, niet wettelijke middelen (zoals bijvoorbeeld onlangs gelanceerd als onderdeel van de EV-campagne) en de samenhang met de mix van andere instrumenten onvoldoende effectief is, is wet- en regelgeving als sluitstuk noodzakelijk. In dit kader zal – onder de bredere kabinetsaanpak EV – worden gemonitord wat de effecten zijn van de campagne onder het bedrijfsleven en dient daarbij te worden geformuleerd wanneer bedrijven 'voldoende effectieve' veiligheidsmaatregelen nemen. In de afweging om over te gaan op wet- en regelgeving en voor welke doelgroep, dient ook rekening te worden gehouden met verschillende typen (sensitieve tech) bedrijven en de verschillende maten waarin zij met economische veiligheid om (kunnen) gaan.

5. Conclusies en aanbevelingen

5.1. CONCLUSIES

De verkenning laat zien dat het integreren van economische veiligheid in de bedrijfsvoering van een bedrijf complex is, ook op het gebied van personeelsbeleid. De dreiging kent verschillende verschijningsvormen en verschillende typen bedrijven hebben verschillende capaciteiten om hiermee om te gaan en daarmee ook te maken met andere (rest)risico's en behoeften aan gerichte ondersteuning.

Maatregelen gericht op voorlichting en bewustwording kunnen als *no regret* worden beschouwd. Het voordeel is een groot bereik maar de daadwerkelijke impact op veiligheid is lager, met name bij kleinere bedrijven zoals startups. Zij hebben gerichte ondersteuning nodig (bijvoorbeeld in de vorm van expertise, middelen en andere beleidsimpulsen) om stappen te kunnen zetten op het gebied van economische veiligheid. Daarbij zou de primaire focus moeten liggen op ontwikkelen, vermarkten en vervolgens beveiligen en compartimenteren van hun intellectueel eigendom, pas dan is het opportuun om ook met personeelsbeleid aan de slag te gaan.

Ondersteuning zou moeten helpen om dit geleidelijk in te kunnen richten, op een manier die de ontwikkeling en opschaling van het bedrijf niet onnodig belemmert. Techbedrijven zijn immers cruciaal voor onze welvaart en bij maatschappelijke uitdagingen, zoals het beschermen van onze veiligheid[14].

In de verkenning is ook gekeken of het opportuun is om wet- en regelgeving in te stellen voor alle sensitieve technologiebedrijven, bijvoorbeeld in de vorm van een zorg- of screeningsplicht. Voor wat betreft de juridische houdbaarheid van een dergelijke wet, is het belangrijk om te kiezen voor een gerichte aanpak die aansluit op hoe bedrijven om (kunnen) gaan met veiligheidsrisico's. Als blijkt dat andere minder vergaande, niet-wettelijke middelen onvoldoende effect hebben, kan dergelijk instrumentarium worden ingezet.

Voor wat betreft een brede screeningsplicht voor alle sensitieve technologiebedrijven, laat de verkenning ook zien dat dit niet voldoende effectief, uitvoerbaar en proportioneel is. Er zijn verschillende kanttekeningen bij de effectiviteit en ook de uitvoerbaarheid staat onder druk, mede als gevolg van de omvang van de doelgroep. Daarmee staan de verwachtte hoge kosten en eventuele neveneffecten niet in verhouding tot de verwachtte extra baten. In de afweging hierbij is ook meegenomen dat bedrijven zelf screenings laten uitvoeren, al dan niet als gevolg van bestaande wet- en regelgeving.

5.2. Aanbevelingen

Het opschalen en verdiepen van initiatieven onder de noemer van de EV-campagne 'Bescherm wat je sterk maakt' kan, zoals eerder benoemd, als *no regret* worden beschouwd. Dit geldt ook voor het voortzetten van de parallelle verkenning, waarbij wordt gekeken of en welke veiligheidsrisico's zich voordoen bij subsidieverstrekking en/ of hoe deze risico's proportioneel gemitigeerd kunnen worden.

Hoewel een screeningsplicht voor alle sensitieve technologiebedrijven niet opportuun wordt geacht, verdient het wel de aanbeveling om binnen de kabinetsbrede aanpak economische veiligheid vanuit beleidsmatig oogpunt verder te onderzoeken waar precies de zorgen zitten op het gebied van ongewenste kennisoverdracht, welke kennis primair zou moeten worden beschermd (bijvoorbeeld op basis van uniciteit of strategische positie in waardeketens) en tegen wie. De verwachting is dat met een andere en gerichtere doelgroepafbakening (een deel van) de kanttekeningen bij de effectiviteit, uitvoerbaarheid en proportionaliteit kunnen worden ondervangen. Of dit ook daadwerkelijk zo is, zal opnieuw moeten worden getoetst bij een nadere doelgroepafbakening. Bovendien is het bij deze vervolgstap belangrijk om integraal te kijken hoe en met welke maatregelen kennis kan worden beschermd, inclusief maatregelen gericht op personeelsbeleid.

[14] Kamerstuk 32 637, nr. 709.

Bijlage 1: quickscan 2024

Hieronder wordt een beknopte weergave gegeven van de quickscan die in 2024 is opgeleverd:

Scope
De verkenning beperkte zich tot risico's op ongewenste kennis- en technologieoverdracht bij de toelating van internationale kenniswerkers van buiten de EU/ EER/ Zwitserland bij in Nederland gevestigde bedrijven die actief zijn op het gebied van sensitieve kennis en technologie. Het streven was daarbij om te focussen op sensitieve technologieën waarvan de risico's voor de nationale veiligheid – als gevolg van ongewenste kennis- en technologieoverdracht – het grootst zijn.

Aanpak
De verschillende handelingsopties zijn – voor zover mogelijk op basis van de toen beschikbare informatie – beoordeeld op de volgende aspecten:

- Doeltreffendheid en doelmatigheid
- Juridische houdbaarheid
- Uitvoerbaarheid
- Neveneffecten voor bedrijven en individuele kenniswerkers
- Proportionaliteit
- Overige randvoorwaarden (o.a. gericht op het al dan niet verstoren van het gelijk speelveld in de Europese Unie).

Onderzochte maatregelen
In de quickscan zijn de volgende maatregelen onderzocht:

- Het actueel houden en intensiveren van bestaande voorlichting en bewustwording als onderdeel van het economisch veiligheidsbeleid;
- Versterkte voorlichting over bestaande exportcontrole- en sanctiewetgeving, *Intangible Technology Transfer* en *Deemed Export*;
- Aanvullende voorwaarden voor erkend referenten (aangaande *pre-employment* screening en aanvullende beveiligingsvoorwaarden ten aanzien van kennisbescherming);
- Het aanwijzen van 'vertrouwensfuncties' bij bedrijven die werken aan sensitieve technologie;
- Aansluiten bij het wetsvoorstel screening kennisveiligheid van OCW;
- Het ontwikkelen van een eigen screeningswet door EZ;
- Screening bij toegang tot de Nederlandse arbeidsmarkt (gekoppeld aan een tewerkstellingsvergunning of een Gecombineerde Vergunning voor Verblijf en Arbeid)
- Versterking van de inlichtingen- en veiligheidsdiensten op het gebied van signalering, screening en voorlichting (flankerend aan bovengenoemde maatregelen).

Conclusies en advies
De maatregelen zijn volgens bovengenoemde aanpak beoordeeld. Het beoordelen van onder andere de uitvoerbaarheid en proportionaliteit bleek echter niet volledig mogelijk, mede omdat de omvang van de doelgroep, evenals de afbakening van sensitieve technologie, onvoldoende scherp was. Bovendien was op dat moment ook duidelijk er nog aandachtspunten waren met betrekken tot de juridische houdbaarheid van maatregelen, met name ten aanzien van screening met het oog op en voorafgaand aan een verblijfsvergunning voor kenniswerkers bij bedrijven. Het advies luidde dan ook om te starten met het verbeteren van de voorlichting aan

bedrijven, maar verdergaande maatregelen pas te overwegen als er meer informatie beschikbaar is over de effectiviteit van maatregelen, het aantal betrokken bedrijven en internationale kenniswerkers, de kosten en potentiële neveneffecten.